Unit 19 Homework: Protecting VSI from Future Attacks

Scenario

In the previous class, you set up your SOC and monitored attacks from JobeCorp. Now, you will need to design mitigation strategies to protect VSI from future attacks.

You are tasked with using your findings from the Master of SOC activity to answer questions about mitigation strategies.

System Requirements

You will be using the Splunk app located in the Ubuntu VM.

Logs

Use the same log files you used during the Master of SOC activity:

- Windows Logs
- Windows Attack Logs
  Apache Webserver Logs
  Apache Webserver Attack Logs

Part 1: Windows Server Attack

Note: This is a public-facing windows server that VSI employees access.

Question 1

- Several users were impacted during the attack on March 25th.
- Based on the attack signatures, what mitigations would you recommend to protect each user account? Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.

  Globally would be to ensure that good security filtering exists at the point of log-on. The purpose of which is to ensure that even the user is being authenticated even before they submit their log on request. Research took me down a rabbit hole regarding Kerberos, NTLM, SASL LDAP. However the main focus to ensure user identity at the point of log on. Individually would be to ensure that employees maintain strong passwords and are changing their password on frequent basis. For example, between 30 - 90 days.

Question 2

- VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.
- What sort of mitigation could you use to protect against this?

  Implement the need for Two-factor authentication. Another strategy would be to incorporate a Captcha.

Part 2: Apache Webserver Attack:

Question 1

- Based on the geographic map, recommend a firewall rule that the networking team should implement.
- Provide a "plain english" description of the rule.
    - For example: "Block all incoming HTTP traffic where the source IP comes from the city of Los Angeles."
- Provide a screen shot of the geographic map that justifies why you created this rule.

  Block all incoming HTTP traffic where source IP comes from Ukraine. As discussed in class however, Geofencing is not so effective. The reason its not as effective as one my assume is due current state of affairs. Currently there is a lot of hacking taking place world wide. Source IPs from Ukraine can be transferred to source IPs in another country.
-

Question 2

- VSI has insider information that JobeCorp will launch the same webserver attack but use a different IP each time in order to avoid being stopped by the rule you just created.

- What other rules can you create to protect VSI from attacks against your webserver?
    - Conceive of two more rules in "plain english".
    - Hint: Look for other fields that indicate the attacker.

      1. If the URI_PATH is to the Log-on page and exceed a threshold amount from an IP, then block

      2.Block IPs where MAC addresses don't match

      3.Drop packets if the rate of the incoming packets is less than a normal time to receive requests.

Guidelines for your Submission:

In a word document, provide the following:

- Answers for all questions.
- Screenshots where indicated

Submit your findings in BootCampSpot!
